Categories of computer crime

Running Head: COMPUTER CRIMES Categories of Computer Crimes School Computer Crimes Modern information technology, such as the internet has initiated new forms of crimes and made perpetration of old felonies effortless. Computer crimes may involve identity theft, cyberstalking, scams and frauds, hacking, creation of malicious codes, child pornography, and violation of copyrights. Criminals use computers to facilitate the embezzlement of money and properties; theft of confidential records; and alteration and destruction of valuable files. The misuse of the computer may involve the falsification of computer signatures through unauthorized codes; the creation of false bank accounts; theft of personal information and misuse of the stolen information; the virus infection created on computers that can hamper the proper software operations and damage records. Today, the biggest crime created through computer use is the electronic financial account transfer (Computer-Based Crime, 2011).

Identity Theft

To date, identity theft has the fastest growing crime rate in America. Identity theft is the pilfering and illegal use of private information from an unsuspecting individual to access personal financial accounts. The targeted personal data include a victim’s address, birth date, telephone number, social security number (SSN), bank account number, credit card number, or other valuable identification records to be used for the thief’s economic gain. Criminals use this information in opening new credit and depository accounts, applying for home or car loans, leasing homes, apartments or vehicles (Brody, Mulig & Kimball, 2007) applying for benefits, or filing fake tax returns (Palmer, 2006). In worst cases, perpetrators use the obtained private information to take over the victim’s identity, create enormous debts,

or use in a criminal activity under the victim’s name (Brody, Mulig & Kimball, 2007).

Phishing Scam

Phishing is a scam that uses volumes of electronic mail messages to attract innocent victims into disclosing private information. A phishing email illustrating a believable problem lures the victim to a fake link that is a replication of the victim’s bank web address; the victim then fixes the imaginary concern and verifies account information and divulges personal identification. Subsequently, the phisher uses the pilfered PIN number, secret code, and identity to drain the victim’s bank account (Brody, Mulig & Kimball, 2007).

Pharming Scam

Pharming is a technically higher form of phishing wherein a virus is unknowingly downloaded on the victim’s computer. The prey keys in a genuine web address but is instead redirected to a mock site. The pharmer then steals the financial account number, password, or other valuable information supplied at the phony web site (ID thieves preying on consumers with new phishing scam called pharming, 2005). Although the preferred web address is shown on the screen, in reality, the domain server system has forwarded the internet traffic to a mere replication of the desired location (Biersdorfer, 2005).

Cyberterrorism

Cyberterrorism is the union of computers, internet and terrorism. In general, it is the unauthorized attack and risk against computers, networks, and the stored information

purposely executed to threaten or force a government, a nation or its people

to advance one’s

political or social intentions. Cyberterrorist attacks demonstrate power and aggressively threaten

or harm persons or property. A perfect example of cyberterrorism is the execution of the

September 11 attack on the World Trade Center (Denning, 2000).

Protective Measures in the Prevention and Mitigation of Computer Crimes

Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) prohibits the distribution of computer code or placement in the market stream if the purpose is to inflict destruction or financial loss. The CFAA centers on a codes destruction to computer systems and the accompanying financial losses, and it charges criminal punishments for either intentional or unintentional release of virus into a business computer system (Hackers: Who’s Responsible?, 2011).

Identity Theft and Assumption Deterrence Act of 1998 (ITADA)

The U. S. Department of Justice acts against identity theft and fraud cases under the 1998 Identity Theft and Assumption Deterrence Act. It prohibits intentional and unauthorized production or transfer of false or stolen identification documents; intentional possession or use of five or more false identification documents; intentional, production, transfer and possession of a document-making equipment that can make false documents; unauthorized or intentional use of stolen United States documents; and intentional and unauthorized use of another person’s identification documents to commit unlawful activity (Identity Theft and Assumption Deterrence Act of 1998, 2011).

Cyberterrorism Defense Initiative (CDI)

The U. S. counter-action against cyberterrorism is the Cyberterrorism Defense Initiative (CDI) which trains technological workforce and executives who monitor and protect the nations important infrastructures. This program educates all levels of public service, as well as the state and local government, the law enforcement and firefighting departments, the public utility sectors, public safety and health institutions, emergency medical services, and education establishments. The training programs are granted free to qualified personnel, and are held in accessible and central locations all over the U. S. (Cyberterrorism Defense Initiative, n. d.).

References

Biersdorfer, J. D. (2005, November 3). As with phishing, shun pharming. New York Times.

Retrieved 12 January 2012 from ProQuest database.

Brody, R. G., Mulig, E., & Kimball, V. (2007, September 1). Phishing, Pharming and Identity

Theft. Academy of Accounting and Financial Studies Journal.

Computer-Based Crime. (2011). Idea Connection. Retrieved 12 January 2012 from:

http://www. ideaconnection. com/solutions/505-Computer-based-crime. html

Cyberterrorism Defense Initiative. (n. d.). Cyberterrorism Center. Retrieved 12 January 2012

from: http://www. cyberterrorismcenter. org/

Denning, D. (2000, May 23). Cyberterrorism. Testimony before the Special Oversight Panel of

Terrorism Committee on Armed Services, US House of Representatives.

Retrieved 12 January 2012 from:

http://www. cs. georgetown. edu/~denning/infosec/cyberter ror. html

Hackers: Who’s Responsible? (2011). WGBH Educational Foundation.

Retrieved 12 January

2012 from: http://www. pbs.

org/wgbh/pages/frontline/shows/hackers/blame/crime

laws. html

Identity Theft and Assumption Deterrence Act of 1998. (2011). National

Check Fraud Center.

Retrieved 12 January 2012 from: http://www. ckfraud. org/title_18. html

ID thieves preying on consumers with new phishing scam called pharming

(2005, October).

PRNewswire. Retrieved 12 January 2012 from:

http://www. nclnet. org/news/2005/phishing_10132005. htm

Palmer, S. (2006, January 10). IRS warns consumers of e-mail scam. St.

Petersburg Times.

Retrieved 12 January 2012 from ProQuest database.